03-06-07

IDW
AF

PATENT

THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	:	Kenneth Aull, et al.
Serial No.	:	10/027,622
Filing Date	:	December 19, 2001
For	:	ASSIGNMENT OF USER CERTIFICATES/PRIVATE KEYS IN TOKEN ENABLED PUBLIC KEY INFRASTRUCTURE SYSTEM
Group Art Unit	:	2137
Examiner	:	Nadia Khoshnoodi
Attorney Docket No.	:	NG(MS)7194

Mail Stop Appeal Briefs - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Sir:

Pursuant to the Notice of Appeal filed in this case on January 4, 2007, Appellant presents this Appeal Brief.

I. TABLE OF CONTENTS

II. REAL PARTY IN INTEREST

The real party in interest is Northrop Grumman Corporation, as indicated by the Assignment recorded July 15, 2004, Reel/Frame: 013751/0849.

III. RELATED APPEAL AND INTERFERENCES

There are no related appeals or interferences.

IV. STATUS OF CLAIMS

Claim 1-16 which are attached in Appendix A, are currently pending in this application. Claims 1-6, 8-14 and 16 stand rejected as being unpatentable under 35 U.S.C §103(a) over U.S. Patent No. 6,194,131 to Geer, Jr. et al. ("Geer") in view of U.S. Patent No. 6,615,171 to Kanevsky et al. ("Kanevsky"). Claims 7 and 15 stand rejected as being unpatentable under 35 U.S.C. §103(a) over Geer and Kanevsky and in further view of U.S. Publication No. 2003/0005291 to Burn ("Burn").

The rejection of claim 1-16 is appealed.

V. STATUS OF AMENDMENTS

A response to a Final Office Action ("Final Rejection") issued on October 6, 2006 was filed on November 7, 2006. No amendments of the claims were filed after the Final Rejection. An Advisory Action Before Filing an Appeal Brief

("Advisory Action") dated November 27, 2006 was issued. The Advisory Action indicated that the request for reconsideration set forth in the Response to the Final Rejection was considered, but did not place the application in condition for allowance.

VI. SUMMARY OF THE CLAIMED SUBJECT MATTER

Claim 1

One aspect of the present invention, as recited in claim 1 is directed to a method for assigning certificates and associated private keys to a token (130 of FIG. 1) (Par. [0031]). The method comprises accessing the token (130 of FIG. 1) through a token reader connected to a computer system (128 of FIG. 1) by a certificate authority (110 of FIG. 1 and 420 of FIG. 4) (Par. [0031]) and reading a token ID and a user signature certificate from the token (130 of FIG. 1 and 430 of FIG. 4) (Par. [0031]). The method also comprises searching for a match for the token ID and the user signature certificate in an authoritative database (104 of FIG. 1 and 440 of FIG. 4) (Par. [0031]) and creating a certificate and an associated private key (450 of FIG. 4) (Par. [0031]), wherein the certificate and the associated private key are wrapped with a public key associated with the token ID and digitally signing the certificate and the associated private key using a signature certificate of the certificate authority (110 of FIG .1) if a match for the token ID and the user signature certificate is found in the authoritative database

(104 of FIG. 1 and 460 of FIG. 4) (Par. [0031]). The method further comprises downloading the certificate and the associated private key to the token (130 of FIG. 1 and 470 of FIG. 4) (Par. [0031]) and decrypting the certificate and the associated private key using a private key stored in the token (130 of FIG. 1) (Par. [0031]), such that the token (130 of FIG. 1) (Par. [0031]) stores at least the token ID, the private key, the user signature certificate and the certificate and the associated private key.

Claim 2

Claim 2 is the method recited in claim 1, wherein the certificate and the associated private key is a plurality of certificates and associated private keys wherein at least one of the plurality of certificates and associated private keys is a signature certificate for the user, an encryption certificate and associated private key for the user, and a role certificate and associated private key for the user (Par. [0029]), wherein the role certificate includes at least one policy (Par. [0024]).

Claim 7

Claim 7 is directed to the method recited in claims 6, wherein decrypting the certificate and the associated private key using the private key stored in the token (130 of FIG. 1) requires the entry of a passphrase by a user (Par. [0029]).

Claim 9

Another aspect of the present invention, as recited in claim 9 is directed to a computer program embodied on a computer readable medium and executable by a computer for assigning certificates and associated private keys to a token (130 of FIG. 1) (Par. [0031]). The computer program comprises accessing the token (130 of FIG. 1) through a token reader connected to a computer system by a certificate authority and reading a token ID and a user signature certificate from the token (130 of FIG. 1 and 430 of FIG. 4) (Par. [0031]). The computer program also comprises searching for a match for the token ID and the user signature certificate in an authoritative database (104 of FIG. 1 and 440 of FIG. 4) (Par. [0031]) and creating a certificate and an associated private key (450 of FIG. 4) (Par. [0031]), wherein the certificate and the associated private key are wrapped with a public key associated with the token ID and digitally signing the certificate and the associated private key using a signature certificate of the certificate authority (110 of FIG. 1) if a match for the token ID and the user signature certificate is found in the authoritative database (104 of FIG. 1 and 460 of FIG. 4) (Par. [0031]). The computer program further comprises downloading the certificate and the associated private key to the token (130 of FIG. 1 and 470 of FIG. 4) (Par. [0031]) and decrypting the certificate and the associated private key using a private key stored in the token (130 of FIG. 1) (Par. [0031]), such that the

token (130 of FIG. 1) (Par. [0031]) stores at least the token ID, the private key, the user signature certificate and the certificate and the associated private key.

Claim 10

Claim 10 is directed to the computer program recited in claim 9, wherein the certificate and associated private key is a plurality of certificates and associated private keys wherein at least one of the plurality of certificates and associated private keys is a signature certificate for the user, an encryption certificate and associated private key for the user, and a role certificate and associated private key for the user (Par. [0029), wherein the role certificate includes at least one policy (Par. [0024).

Claim 15

Claim 15 is directed to the computer program recited in claim 14, wherein the decrypting the certificate and the associated private key using the private key stored in the token (130 of FIG. 1) requires the entry of a passphrase by a user (Par. [0029]).

VII. GROUNDS OF REJECTION TO BE REVIEW ON APPEAL

A. Whether claims 1-6, 8-14 and 16 are made obvious by Geer in view of Kanevsky?

B. Whether claims 7 and 15 are made obvious by Geer in view of Kanevsky and in further view of Burn?

VIII. ARGUMENTS FOR CLAIMS 1-16

The Court of Customs and Patent Appeals has held that to establish prima facie obviousness of a claimed invention, all the claimed limitations must be taught or suggested by the prior art. *In re Royka*, 490 F.2d 981, 180 U.S.P.Q. 580 (C.C.P.A. 1974).

A. 35 U.S.C. §103(a) rejection of claims 1-6, 8-14 and 16 as being unpatentable over Geer in view of Kanevsky

1. The Obviousness Rejection of claims 1 and 9

a. Geer taken in view of Kanevsky does not teach or suggest accessing a token through a token reader connected to a computer system by a certificate authority, as recited in claims 1 and 9.

Geer taken in view of Kanevsky does not teach or suggest accessing a token through a token reader connected to a computer system by a certificate authority, as recited in claims 1 and 9. In the Final Rejection, the Examiner contended that Column 2, Lines 27-39 of Geer discloses this element of claims 1 and 9 (See Final Rejection, Page 5). Applicant's representative respectfully disagrees. The cited section of Geer discloses that a smart card at an authorizing computer 10 is initialized by the creation of a public key pair for the smart card and a public key pair for the user of the card (See Geer, Col. 2, Lines 40-45). The cited section of Geer also discloses that a certifying authority 18

performs the conventional function of certifying the identity of the user to authorized computer 14 and transaction computer 16 (See Geer, Col. 2, Lines 36-39).

Geer does not teach or suggest that the disclosed certifying authority 18 can access a token, in contrast to the certificate authority recited in claims 1 and 9. Instead, Geer discloses that a user is verified by authorizing computer 10 sending the authorized computer 14 an identification certificate signed with the private key of the certifying authority 18, and the authorized computer 14 verifies the authenticity of the signature on the identification certificate (See Geer, Col. 2, Lines 50-60). That is, in claims 1 and 9, the certificate authority access the token, while in Geer, identity is verified by passing the identification certificate from the authorizing computer 10 to the authorized computer 14, and to the certifying authority 18.

In the Advisory Action, the Examiner contended that Geer teaches that the certifying authority 18 must have access to a user's information via the smart card in order to be able to prove the user's identity to computers that the user is requesting some type of service from. Applicant's representative respectfully submits that access by the certifying authority 18 to the user information via the smart card is neither explicitly disclosed nor suggested by Geer. As stated above, in Geer, a user is verified by the authorizing computer 10 sending the authorized computer 14 an identification certificate. Such an implementation

would not require that the certifying authority 18 access user information via the disclosed smart card, because the identification certificate is provided by another entity (the authorizing computer 10). Additionally, in such a situation, the authorizing computer 10 would be susceptible to malicious code (e.g., computer viruses) that could intercept the identification certificate. Claim 1 overcomes this security issue of Geer. Specifically, in claim 1, since the token includes a private key, data can be transferred to and from the token securely. That is, in claim 1, even if an unauthorized user (e.g., a hacker) were to obtain information (e.g., by malicious code) that originated from, or was destined for the token; the information would be useless, since the hacker would not have the private key of the token. Accordingly, Geer taken in view of Kanevsky does not teach or suggest accessing a token through a token reader connected to a computer system by a certificate authority, as recited in claims 1 and 9.

b. Geer taken in view of Kanevsky does not teach or suggest downloading a certificate and an associated private key to a token, as recited in claims 1 and 9, when claims 1 and 9 are read as a whole.

Geer taken in view of Kanevsky does not teach or suggest downloading a certificate and an associated private key to a token, as recited in claims 1 and 9, when claims 1 and 9 are read as a whole. In the Final Rejection, the Examiner contended that Geer discloses downloading a certificate and an associated private key to a token (See Final Rejection, Page 3, Citing Geer, Col. 6, Lines 15-

27). Applicant's representative respectfully disagrees with this contention. The U.S. Court of Appeals for the Federal Circuit ("Federal Circuit") has held that the determination of obviousness requires an evaluation of the claimed invention *as a whole*, and not merely the differences between the claimed invention and the prior art (emphasis added). *Lear Siegler, Inc. v. Aeroquip Corp.*, 733 F.2d 881, 221 U.S.P.Q. 1025, 1033 (Fed. Cir. 1984). Applicant's representative respectfully submits that in rejecting claims 1 and 9, the Examiner is not considering claims 1 and 9, as a whole.

Specifically, when claims 1 and 9 are read as a whole, it is clear that the certificate is downloaded to a token that is the same token from which a user-signature certificate is read. In the Final Rejection, the Examiner contends Column 2, Lines 51-60 of Geer discloses reading a user-signature certificate from a token (See Final Rejection, Page 5). The cited section of Geer discloses that an authorizing computer 10 sends an authorized computer 14 a public key certificate (e.g., an identification certificate) identifying a user and the user's public key (See Geer, Col. 2, Lines 51-55).

Even assuming *arguendo* that an identification certificate is similar to a signature certificate, Geer still fails to teach or suggest the downloading recited in claims 1 and 9. The section of Geer that the Examiner contends discloses the downloading recited in claims 1 and 9, discloses that the authorizing computer 10 sends an authorization certificate to a smart card at the authorized computer 14

that interacts with a program stored at the authorized computer 14 (See Geer, Col. 6, Lines 7-10). That is, the smart card at the authorized computer 14 is a different smart card than the smart card from which the identification certificate is provided.

While Geer does disclose that the authorized computer 14 sends a public key certificate to the authorizing computer 10 identifying the user of the authorized computer 14 (See Geer, Col. 2, Lines 60-63), Geer fails to teach or suggest that the public key certificate is ever stored on a smart card at the authorized computer 14. In fact, in the section of Geer that the Examiner contends discloses the downloading recited in claims 1 and 9 discloses that interaction with the smart card at the authorized computer 14 occurs when the authorized computer 14 contains a program that requires a license or a program fragment to function (See Geer, Col. 6, Lines 10-14). The cited section of Geer is not related to identification of the user of the authorized computer 14. Thus, the sending of an authorization certificate to a smart card at the authorization computer 14 does not correspond to the downloading recited in claims 1 and 9. Accordingly, Geer taken in view of Kanevsky does not teach or suggest downloading a certificate and an associated private key to a token, when claims 1 and 9 are read as a whole.

c. Geer taken in view of Kanevsky does not teach or suggest searching for a match for the token ID and the user signature certificate in an authoritative database, and that a certificate and an associated private key are wrapped with a public key associated with the token ID if a match is found for the token ID and the user signature certificate is found in the authoritative database, as recited in claims 1 and 9.

In the Final Rejection, the Examiner admitted that Geer does not teach or suggest searching for a match for the token ID and the user signature certificate in an authoritative database, and that a certificate and an associated private key are wrapped with a public key associated with the token ID if a match is found for the token ID and the user signature certificate is found in the authoritative database, as recited in claims 1 and 9 (See Final Rejection, Page 5). In fact, Applicant's representative respectfully asserts that Geer is silent on a token (e.g., a smart card), having a token ID, in contrast to claims 1 and 9. Additionally, Applicant's representative respectfully submits that the addition of Kanevsky does not make up for the deficiencies of Geer.

In the Final Rejection, the Examiner cited Col. 8, Lines 29-46 of Kanevsky in the rejection of claims 1 and 9. The cited section of Kanevsky discloses that if a user forgets his personal identification number (PIN) or if his PIN expires without being reset that the user can reestablish his PIN by linking to an automatic speech/speaker recognition (ASSR) server 200 via a communication

link to request a PIN reset through a personal computer 450 and a smart card reader 460 (See Kanevsky, Col. 8, Lines 21-28). Kanevsky also discloses that a user provides his user ID, name and smart card serial number to the ASSR server 200 (See Kanevsky, Col. 8, Lines 31-34). Kanevsky further discloses that the ASSR server 200 accesses a stored certificate and the ASSR server 200 uses the smart card's certificates and public key to encrypt a PIN reset command, which is activated by the smart card (See Col. 8, Lines 35-47).

Kanevsky does not teach or suggest that a certificate and an associated private key are wrapped with a public key associated with a token ID, as recited in claims 1 and 9. Instead, Kanevsky discloses that a PIN reset command is encrypted with a smart card's certificate and public key. Clearly, the PIN reset command does not correspond to the certificate recited in claims 1 and 9. Accordingly, taken individually or in combination, Geer and Kanevsky do not teach or suggest each and every element of claims 1 and 9.

d. There is no motivation to combine and modify the teachings of Geer and Kanevsky in the manner suggested by the Examiner.

There is no motivation to combine and modify the teachings of Geer and Kanevsky in the manner suggested by the Examiner. The Federal Circuit has held that trade-offs concern what is feasible, while motivation to combine requires what is desirable. *Winner Int'l Royalty Corp. v. Ching-Rong Wang* 202 F.3d 1340, 1349, 53 U.S.P.Q.2d 1580 (Fed. Cir. 2000). In *Winner*, the Federal

Circuit held that one of ordinary skill in the art would not have reasonably elected trading the benefit of security for that of convenience. 202 F.3d 1340, 1349, 53 U.S.P.Q.2d 1580.

Geer does not even mention the employment of token IDs (e.g., smart card IDs), as recited in claims 1 and 9. Applicant's representative respectfully submits that if the system disclosed in Geer were modified to employ smart card IDs in the manner suggested by the Examiner, particular smart cards (e.g., tokens) would need to be assigned to particular users and computers in an authoritative database. That is, the smart cards would not be generic or transferable (e.g., by copying contents of the smart card). There is no motivation in Geer to employ such a system, as employing token IDs would result in a less convenient system. One skilled in the art would not be motivated to tradeoff the benefit of using a generic smart card for the increased security and complexity of a system where the smart cards were assigned to particular users and computers. Thus, there is no motivation to combine and modify the teachings of Geer and Kanevsky in the manner suggested by the Examiner.

Accordingly, for the reasons stated above, Geer taken in view of Kanevsky does not make claims 1 and 9 obvious. Therefore, claims 1 and 9 should be patentable. Thus, it is respectfully requested that the rejection of claim 1 be withdrawn.

2. The Obviousness Rejection of Claims 2 and 10

a. Geer taken in view of Kanevsky does not teach or suggest that a certificate and an associated private key is a plurality of certificates and associated private keys, wherein at least one of the certificates and associated private keys is a signature certificate for a user, an encryption certificate for the user and a role certificate and associated private key for the user, wherein the role certificate includes at least one policy, as recited in claims 2 and 10.

Claims 2 and 10 depend from claims 1 and 9, respectively, and are patentable for at least the same reasons as claims 1 and 9, and for the reasons given herein.

Geer taken in view of Kanevsky, does not teach or suggest that a certificate and an associated private key is a plurality of certificates and associated private keys, wherein at least one of the certificates and associated private keys is a signature certificate for the user, an encryption certificate and associated private key for the user, and a role certificate and associated private key for the user, wherein the role certificate includes at least one policy, as recited in claims 2 and 10. Claims 2 and 10 define properties of the certificate recited in claims 1 and 9 that is downloaded to a token. In rejecting claims 2 and 10, the Examiner cites Col. 3, Lines 29-33 of Geer. Geer discloses that an authorization certificate is generated by a smart card on an authorizing computer

10 (See Geer, Col. 3, Lines 23-24) and the smart card signs the authorization certificate with the private key of the smart card (See Geer Col. 3, Lines 33-34). Geer also discloses that the authorizing computer 10 sends the authorization certificate to a smart card at authorized computer 14 (See Geer, Col. 6, Lines 8-10). However, since claims 2 and 10 depend from claims 1 and 9, respectively, the certificate recited in claims 2 and 10 is downloaded to the token, which is the same token from which a user signature certificate is read.

For the reasons stated above, Geer taken in view of Kanevsky does not teach or suggest reading a token ID and a user-signature certificate from a token and downloading a certificate and associated private key to the same token, as recited in claims 1 and 9, from which claims 2 and 10 depends. Therefore, Geer taken in view of Kanevsky does not teach or suggest specific properties of the certificate that is downloaded to the token, as recited in claims 2 and 10. Thus, Geer taken in view of Kanevsky does not make claims 2 and 10 obvious, and the rejection of claims 2 and 10 should be withdrawn.

3. The Obviousness Rejection of Claims 3-6, 8, 11-14 and 16

Claims 3-6, 8, 11-14 and 16 depend either directly or indirectly from claims 1 and 9 and are patentable for at least the same reasons as claims 1 and 9, and for the specific elements recited therein. Accordingly, the rejection of claims 3-6, 8, 11-14 and 16 should be withdrawn.

B. 35 U.S.C. §103(a) rejection of claims 7 and 15 as being unpatentable over Geer in view of Kanevsky and in further view of Burn

1. The Obviousness Rejection of claims 7 and 15

a. The teachings of Geer, Kanevsky and Burn teach away from their combination and modification in the manner suggested by the Examiner, because the purported combination would result in an inoperable device.

Claims 7 and 15 depend from claims 1 and 2, and 9 and 10. Accordingly, claims 7 and 15 are patentable for at least the same reasons as claims 1, 2, 9 and 10, and for the reasons given herein.

In the Final Rejection, the Examiner admitted that Geer taken in view of Kanevsky does not teach or suggest that decrypting a certificate and associated private key using a private key stored in a token requires the entry of a passphrase, as recited in claim 7 and 15 (See Final Rejection, Page 8). In an attempted to cure the deficiencies of Geer taken in view of Kanevsky, the Examiner cited Burn. Applicant's representative respectfully submits that Geer, Kanevsky and Burn teach away from their respective combination and modification in the manner suggested by the Examiner in the Final Rejection. The Federal Circuit has held that references teach away from their combination if the references taken in combination would produce a seemingly inoperable device. *McGinley v. Franklin Sports Inc.*, 262 F.3d 1339, 1354, 60 U.S.P.Q.2d 1001, 1010 (Fed. Cir. 2001). In Kanevsky, the only reasons taught or suggested

for sending a PIN reset command, as discussed above with respect to claims 1 and 9, is when a user forgets his PIN or the PIN has expired (See Kanevsky, Col. 8, Lines 21-23). Accordingly, a user in such a situation would not be able to enter a PIN, as either the user would not know the PIN, or the PIN would be expired. In contrast, claims 7 and 15 require that a passphrase be entered by a user. If the teachings of Geer and Kanevsky were combined and modified with Burn such that a user were required to enter a PIN when the user forgot his PIN or the PIN were expired, the user would not be able to decrypt the PIN reset command, since that user would not be able to remember his PIN, or the PIN would no longer be valid (e.g., expired).

In the Final Rejection, the Examiner contended that Kanevsky discloses several reasons for sending the PIN reset command (See Final Rejection, Page 4, citing Col. 8, Lines 21-31). However, the cited section of Kanevsky only discloses the two reasons discussed above, namely, if the user forgot his PIN or if the PIN has expired without resetting. As stated above, in either case, the user would not be able to decrypt the PIN reset command. Accordingly, Applicant's representative respectfully submits that combining and modifying the teachings of Geer, Kanevsky and Burn in the manner suggested by the Examiner would result in an inoperable device, and thus, the references teach away from their combination.

Accordingly, for the reasons stated above, Geer taken in view of Kanevsky and in further view of Burn does not make claims 7 and 15 obvious. Therefore, claims 7 and 15 should be patentable. Thus, it is respectfully requested that the rejection of claims 7 and 15 be withdrawn.

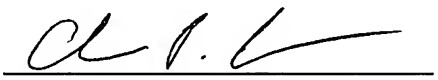
IX. APPENDICES

The first attached Appendix contains a copy of the claims on appeal.

The second and third Appendices have been included to comply with statutory requirements.

Please charge any deficiency or credit any overpayment in the fees for this Appeal Brief to Deposit Account No. 20-0090.

Respectfully submitted,



Christopher P. Harris
Reg. No. 43,660

TAROLLI, SUNDHEIM, COVELL
& TUMMINO, L.L.P.
1300 East Ninth Street, Suite 1700
Cleveland, Ohio 44114
(216) 621-2234
(216) 621-4072 (Facsimile)
Customer No.: 26294

Claims Appendix

Claim 1 A method for assigning certificates and associated private keys to a token, comprising:

accessing the token through a token reader connected to a computer system by a certificate authority;

reading a token ID and a user signature certificate from the token;

searching for a match for the token ID and the user signature certificate in an authoritative database;

creating a certificate and an associated private key, wherein the certificate and the associated private key are wrapped with a public key associated with the token ID and digitally signing the certificate and the associated private key using a signature certificate of the certificate authority if a match for the token ID and the user signature certificate is found in the authoritative database;

downloading the certificate and the associated private key to the token; and

decrypting the certificate and the associated private key using a private key stored in the token, such that the token stores at least the token ID,

the private key, the user signature certificate and the certificate and the associated private key.

Claim 2 The method recited in claim 1, wherein the certificate and the associated private key is a plurality of certificates and associated private keys wherein at least one of the plurality of certificates and associated private keys is a signature certificate for the user, an encryption certificate and associated private key for the user, and a role certificate and associated private key for the user wherein the role certificate includes at least one policy.

Claim 3 The method recited in claim 2, wherein the wrapping of the certificate and the associated private key with the public key of the token encrypts the certificate and the associated private key.

Claim 4 The method recited in claim 3, wherein the token is a smart card.

Claim 5 The method recited in claim 4, wherein the token ID is assigned by a token manufacturer at the time the token is created and stored in the authoritative database when assigned to a user.

Claim 6 The method recited in claim 5, wherein downloading the certificate and the associated private key to the token is done through an unsecured communications line.

Claim 7 The method recited in claim 6, wherein decrypting the certificate and the associated private key using the private key stored in the token requires the entry of a passphrase by a user.

Claim 8 The method recited in claim 7, further comprising:

authenticating, by the signing of the certificate and the associated private key using a signature certificate of the certificate authority, that the certificate and the associated private key were issued by the certificate authority.

Claim 9 A computer program embodied on a computer readable medium and executable by a computer for assigning certificates and associated private keys to a token, comprising:

accessing the token through a token reader connected to a computer system by a certificate authority;

reading a token ID and a user signature certificate from the token;

searching for a match for the token ID and the user signature certificate in an authoritative database;

creating a certificate and an associated private key, wherein the certificate and the associated private key are wrapped with a public key associated with the token ID and digitally signing the certificate and the associated private key using a signature certificate of the certificate authority if a match for the token ID and the user signature certificate is found in the authoritative database;

downloading the certificate and the associated private key to the token; and

decrypting the certificate and the associated private key using a private key stored in the token, such that the token stores at least the token ID, the private key, the user signature certificate and the certificate and the associated private key.

Claim 10 The computer program recited in claim 9, wherein the certificate and associated private key is a plurality of certificates and associated private keys wherein at least one of the plurality of certificates and associated private keys is a signature certificate for the user, an encryption certificate and associated private key for the user, and a role certificate and associated private key for the user, wherein the role certificate includes at least one policy.

Claim 11 The computer program recited in claim 10, wherein the wrapping of the certificate with the public key of the token encrypts the certificate and the associated private key.

Claim 12 The computer program recited in claim 11, wherein the token is a smart card.

Claim 13 The computer program recited in claim 12, wherein the token ID is assigned by a token manufacturer at the time the token is created and stored in the authoritative database when assigned to a user.

Claim 14 The computer program recited in claim 13, wherein downloading the certificate and the associated private key to the token is done through an unsecured communications line.

Claim 15 The computer program recited in claim 14, wherein the decrypting the certificate and the associated private key using the private key stored in the token requires the entry of a passphrase by a user.

Claim 16 The computer program recited in claim 15, further comprising:

authenticating by the signing the certificate and the associated private key using a signature certificate of the certificate authority that the certificate and the associated private key was issued by the certificate authority.

Evidence Appendix

None

Related Proceedings Appendix

None